**OpenDJ Password Policy**

**Video links:**

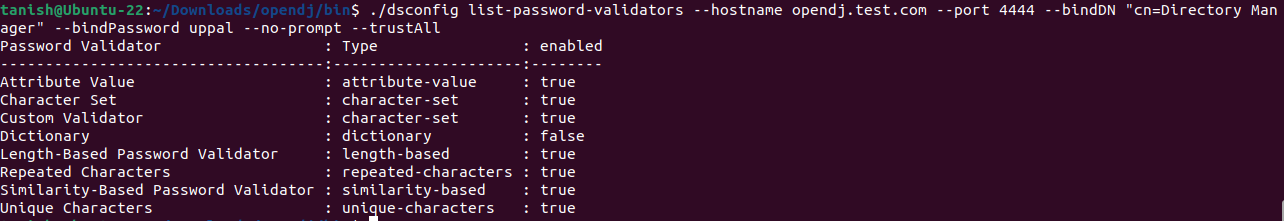
* <https://www.youtube.com/watch?v=vo1GO4eppzY&list=PLWUs-qjlPXmlx6gkb4bWQrIQizspT2Z7p&index=9>
* <https://www.youtube.com/watch?v=ZHAplhgTrWI&list=PLWUs-qjlPXmlx6gkb4bWQrIQizspT2Z7p&index=10>
* <https://www.youtube.com/watch?v=5FCQafvq81A&list=PLWUs-qjlPXmlx6gkb4bWQrIQizspT2Z7p&index=8>

In this example, we will set password policy such as user must have atleast 1 smallcase letter,1 uppercase letter,1 number,1 alphanumeric character and min length should be 8 and max length should be 14.

**Steps:**

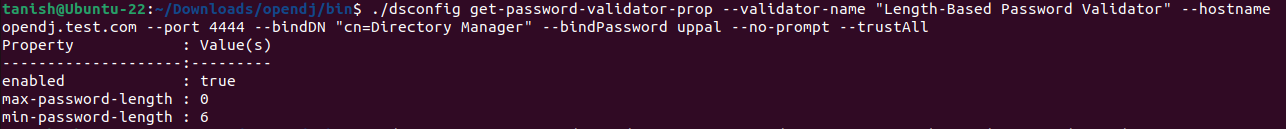
1. Go into bin folder inside opendj.In this example opendj is kept installed in Downloads: cd /Downloads/opendj/bin
2. OpenDJ has many default Password Validators. Check them by command:

./dsconfig list-password-validators --hostname opendj.test.com --port 4444 --bindDN "cn=Directory Manager" --bindPassword uppal --no-prompt –trustAll



1. Now we have to update length based constraints. So let’s check length-based password validator:

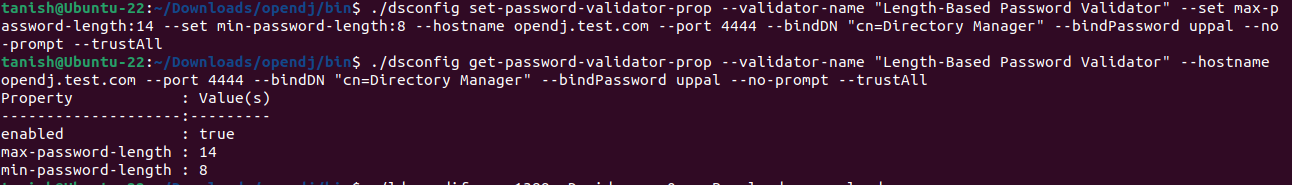
./dsconfig get-password-validator-prop --validator-name "Length-Based Password Validator" --hostname opendj.test.com --port 4444 --bindDN "cn=Directory Manager" --bindPassword uppal --no-prompt –trustAll



1. Now let’s change the max-length to 14 and min-length to 8:

./dsconfig set-password-validator-prop --validator-name "Length-Based Password Validator" --set max-password-length:14 --set min-password-length:8 --hostname opendj.test.com --port 4444 --bindDN "cn=Directory Manager" --bindPassword uppal --no-prompt –trustAll

1. Now check if the parameters have been changed or not by running same command as in step number 3



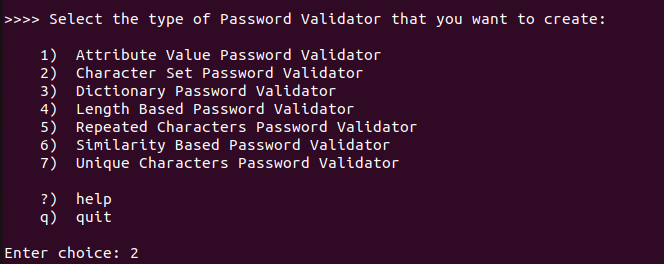
Note: These changes in default Password Validators will not get into effect just by changing, we will apply them in policy later.

1. Now let’s create a custom password validator that will check the condition that password contains atleast 1 smallcase letter, 1 uppercase letter,1 number, 1 alphanumeric character
2. Run command:

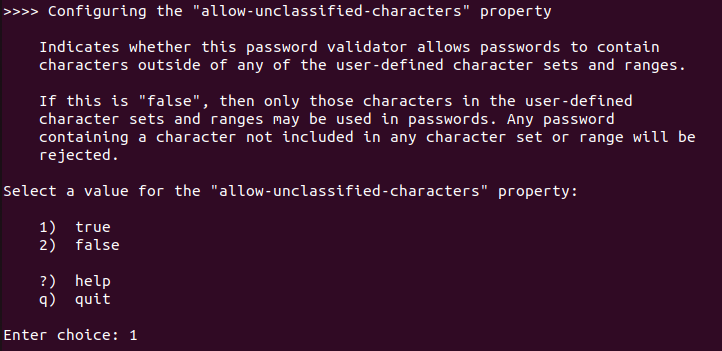
./dsconfig create-password-validator --hostname opendj.test.com --port 4444 --bindDN "cn=Directory Manager" --bindPassword uppal --validator-name "Custom Validator"



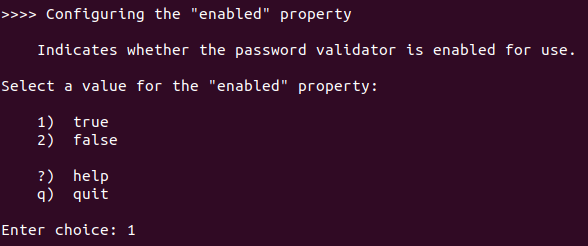
1. It will ask the type of validator you want to create. In this example we are creating character set password validator



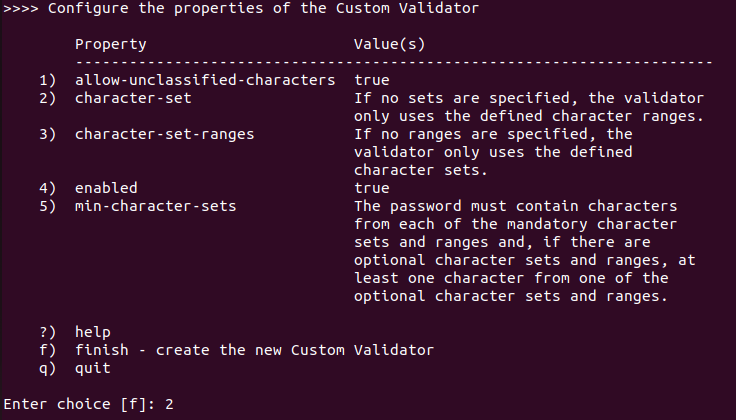
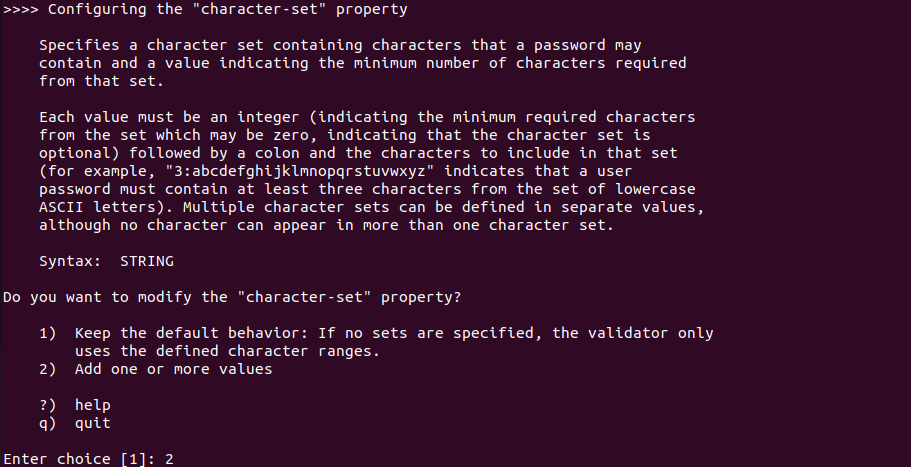
Next it is asking whether you want to allow passwords to contain characters outside of any of the user-defined character sets and ranges. We will choose true



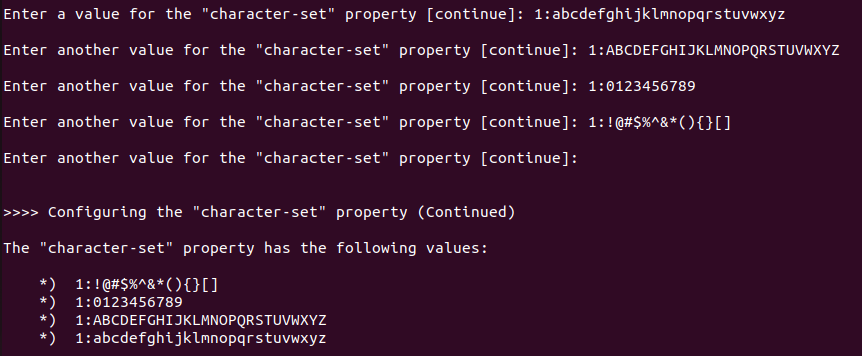
Next it is asking to enable this validator for use or not. So we will choose true as we will apply this validator in password policy.



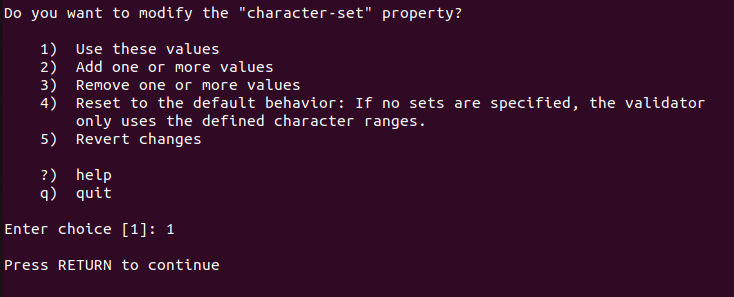
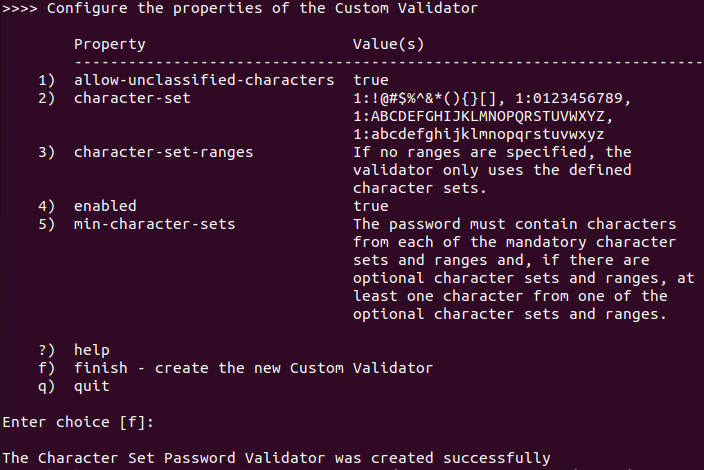
Next we have to define character sets from which password must contain atleast 1 element



Now we have defined the character sets as seen in below screenshot

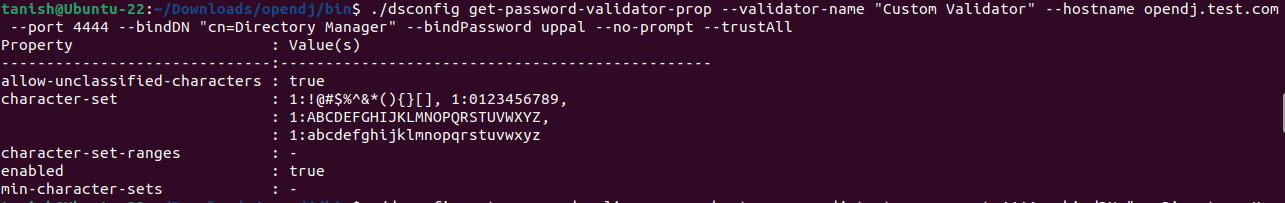


Let’s apply these changes and hit finish to create this custom validator



1. Let’s check the custom validator we just created:

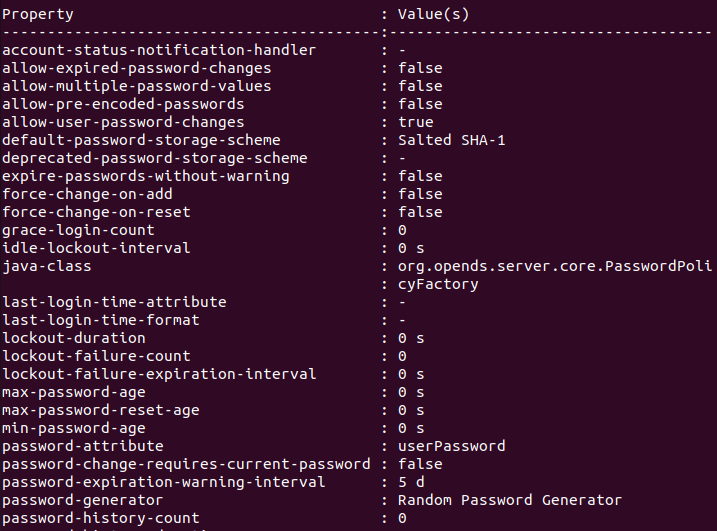
./dsconfig get-password-validator-prop --validator-name "Custom Validator" --hostname opendj.test.com --port 4444 --bindDN "cn=Directory Manager" --bindPassword uppal --no-prompt –trustAll

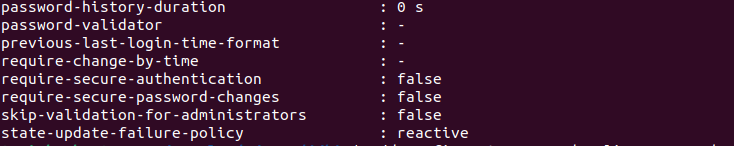


Now it’s time to put this validator in use.

1. Now let’s check all the attributes which Default Password Policy consists of:

./dsconfig get-password-policy-prop --hostname opendj.test.com --port 4444 --bindDN "cn=Directory Manager" --bindPassword uppal --policy-name "Default Password Policy" –advanced

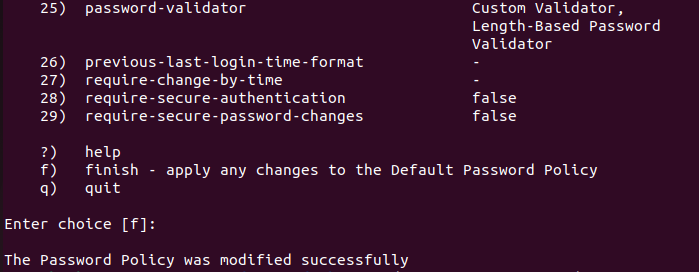




Changing these attributes will cahnge the password policy for OpenDJ

1. Now let’s add our validators(length validator and custom validator) in password-validator attribute

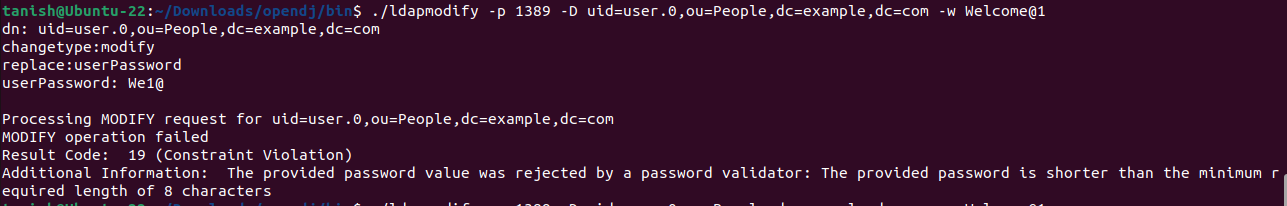
/dsconfig set-password-policy-prop --hostname opendj.test.com --port 4444 --bindDN "cn=Directory Manager" --bindPassword uppal --policy-name "Default Password Policy" --set password-validator:"Custom Validator" --set password-validator:"Length-Based Password Validator"



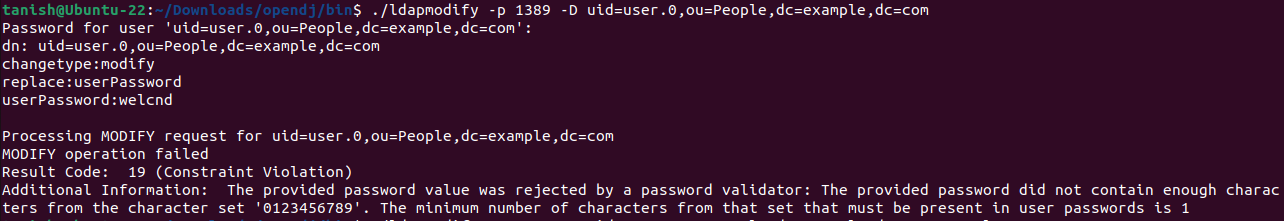
As you can see, our validators have been applied in password policy.

1. You can also confirm by running same command as in step 10
2. Now you can test by creating new user or by changing password of any user in ldap
3. Here I am testing on user having uid=user.0 having password Welcome@1.

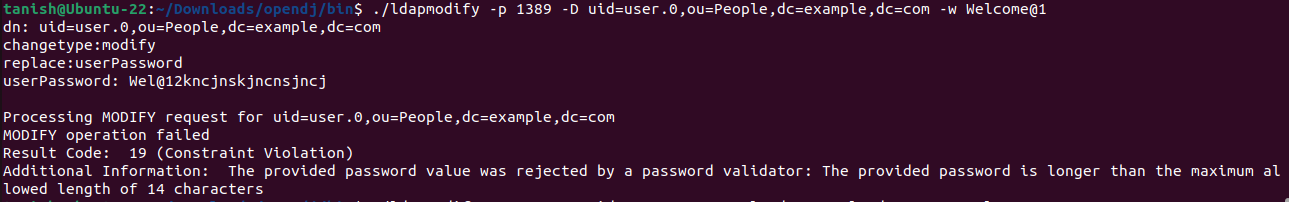
Test 1:



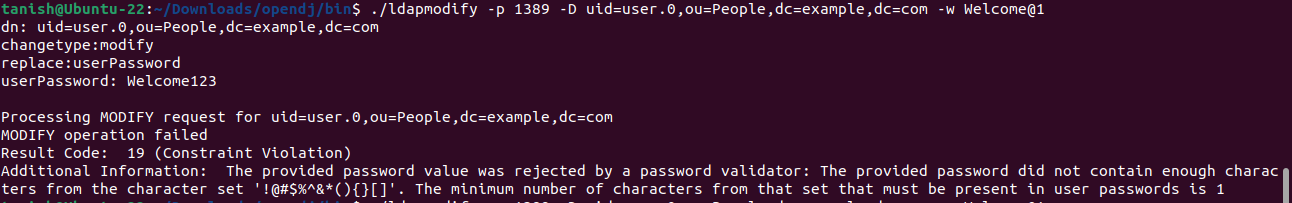
Test 2:



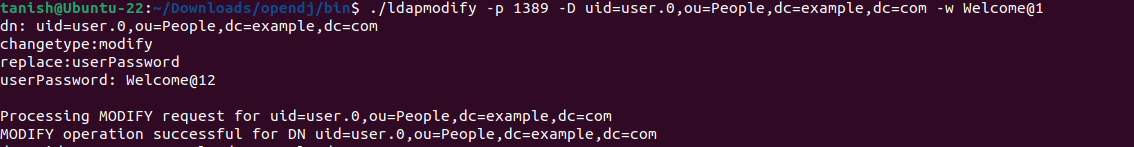
Test 3:



Test 4:



Test 5:



------- THANK YOU -------